ALISON ADIELISON DIONATO DA SILVA

MANUAL DE SEGURANÇA NA INTERNET:
Algumas breves dicas de como ter um acesso mais seguro a internet

Jales
2018

INTRODUÇÃO

Atualmente a internet é maior meio de comunicação utilizado no mundo, bilhões de habitantes a utilizam diariamente, e como todos sabemos, a rede das redes possui uma parte perigosa que muitos usuários desconhecem, e por essa ignorância da partes deles, pessoas se aproveitam e acabam roubando dados importantes como: dados pessoais, senhas, contas de banco e etc., e os receptores dessas ações criminosas acabam sendo prejudicados, seja moralmente, psicologicamente ou financeiramente.

Este é um manual de segurança na internet, realizado de acordo com pesquisas feitas na internet, e com o conteúdo que nos foi passado em sala de aula na disciplina de Bases de Internet pelo Prof. Virgílio Muller, com o intuito de avisar aos utilizadores de internet sobre os possíveis riscos que eles correm, mas também, informa-los de que simples ações podem os proteger e com isso evitar com que sofram por crimes realizados virtualmente.

Espero por meio desta cartilha, ajudar aos leitores a se prevenir de possíveis ameaças que a internet possui subliminarmente, ou em alguns casos, explicitamente, mas que infelizmente não todos têm acesso a essa informação, portanto, acredito que após o termino da leitura, o leitor possa estar ciente de que a internet pode ser um lugar perigoso se usado sem cautela, e que existem pessoas dispostas a fazer o mau ao próximo para se beneficiar ou até apenas para causar dor, tristeza aos envolvidos.

Simples ações que muitas vezes parecem ser inofensivas ou não demonstram ser importantes, podem até mesmo lhe salvar um ataque cibernético, ou seja, pequenas atitudes que muitos deixam de tomar, podem acarretar grandes e más consequências.

DESENVOLVIMENTO

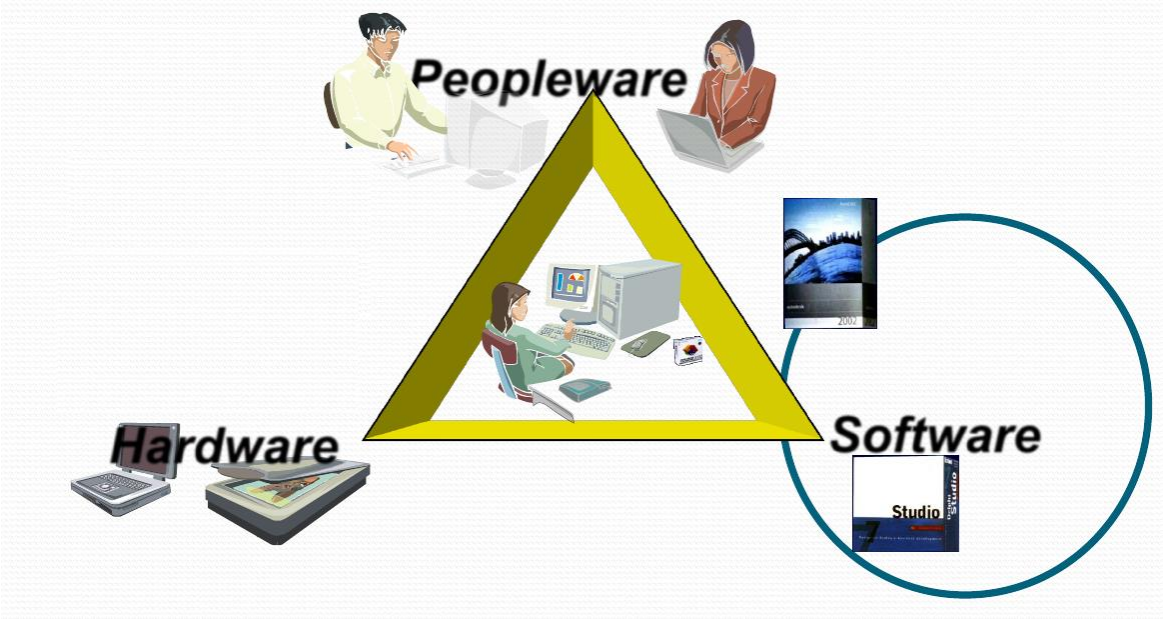
Dados de Acesso

Atualmente, o mundo possui cerca de 7,6 bilhões de habitantes, distribuídos pelos seus 5 continentes habitáveis, e você já se perguntou quantas pessoas possuem acesso a internet? Bom, se sua resposta for próxima de metade da população você está certo, porque uma pesquisa feita pelos serviços online Hootsuite e We Are Social, aponta que em janeiro de 2018, mais de 4 bilhões de pessoas têm acesso a internet, tendo as redes sociais com a maior parte desses acessos com 3,2 bilhões de usuários, e o ponto de acesso mais utilizado são os smartphones com 52% dos acessos, enquanto os desktops e notebooks têm 43%.

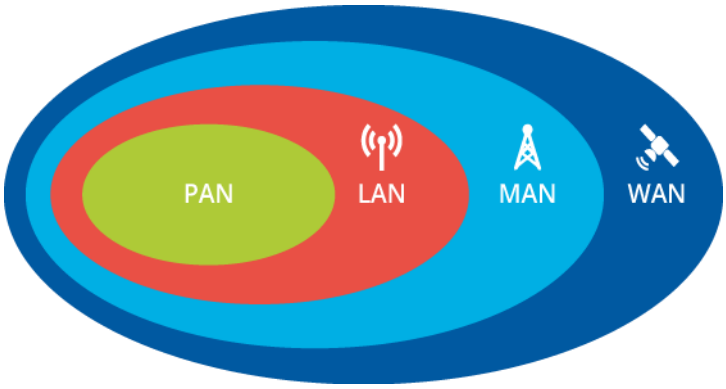
O que é a Internet?

A internet é o maior meio de comunicação do mundo, ela pode ser caracterizada como a “rede das redes”, pois é um conjunto de redes menores que se ligam através de diversas formas e dão origem a internet, tendo impacto global.

A internet é composta por 4 componentes: Peopleware (usuário que irá utilizar a rede), Hardware (a parte física, tangível, que formam as redes: Servidores, cabos, antenas, computadores, modem, etc.), Software (responsável por fazer a interação do usuário com o hardware, por meio de um sistemas operacional base, dotado por outros programas com fins específicos), Protocolos(regras e acordos gerados para possibilitar a troca de informações entre os usuários e redes, e por meio deles, garantir também uma certa segurança, os mais conhecidos são: TCP/IP, HTTP, FTP, etec.).



Quando se trata de redes, 4 tipos são os predominantes, estes são: PAN ou Personal Area Network (trata-se de uma rede pessoal), LAN ou Local Area Network (rede local, pode ser um edifício, uma sala ou até mesmo um campus, podendo se estender até de 10m a 10km), MAN ou Metropolitan Area Network (rede de uma cidade, exemplo: os provedores de internet locais utilizam esse tipo de rede em seus serviços podendo alcançar de 10km a 100km entre os hosts), WAN ou Wide Area Network (rede geograficamente distribuída de um país, ou continente, podendo ter de 100km a 10.000km entre distância dos hosts), partir de 10.000km é a Internet global, host é qualquer dispositivo que se conecta a algum tipo de rede.



Como surgiu a Internet?

A internet surgiu no século XX, após a Guerra Fria com o surgimento da ARPANET que tinha como objetivo na época, proteger as informações do governo dos EUA caso sofresse um ataque direto, pois se uma das conexões fosse atacados, os dados permaneceriam protegidos em outros local, porque o tráfego de dados podia ser automático para outras conexões.

A internet que conhecemos foi criada por Tim Berners Lee, que propôs um projeto onde as pessoas poderiam compartilhar e cominar seus dados e conhecimentos em uma única rede de documentos por meio de um hipertexto, esse projeto ficou conhecido como World Wide Web (teia global). A WEB só ficou disponível mundialmente a partir do verão de 1991.

Quais são os riscos?

Como todos sabemos, a internet “move o mundo”, e atualmente a falta dela traria grandes problemas para toda a economia mundial, além de todos os benefícios que nos foi concebido pela rede mundial de computadores, mas, existem alguns riscos que em alguns casos são desconhecidos pelos usuários, esses são:

O acesso a conteúdo indevidos ou ofensivos:

- Sites pornográficos, conteúdo nazista.

Contato com pessoas mau intencionadas:

- Estupradores, psicopatas, pedófilos, assassinos, e alguns casos seriais killers.

Furto de identidade:

- Não compartilhe dados importantes com pessoas que foram conhecidas pela internet, pois podem ser criminosos e você pode ter seus dados roubados, e ser muito prejudicado principalmente financeiramente.

Furto e perda de dados:

- Todas as informações que ficam armazenados em computadores ou qualquer dispositivo que tenha acesso a internet, pode ser apagado, furtado, e alterados por meio de softwares que podem ser acoplados em nos aparelhos sem que o usuário perceba.

Invasão de privacidade:

- Compartilhar muitos dados pessoais pode ser algo ruim, exemplo disso são alguns utilizadores de uma certa rede social que preenchem todas as informações a seu respeito, até mesmo fatos que parecem ser inofensivos, na mão de pessoas más intenções pode ser perigoso.

Fake News:

- Esse é um assunto muito atual, o que seria fake News? São boatos, notícias a respeito de algo ou alguém que é mentira, e por causa de ter sido postado na internet, a repercussão é rápida e atinge um grande público, que muitas vezes acreditam na tal notícia.

Exclusão quase impossível:

- Informações jogadas na internet, são muito difíceis de serem apagadas, maioria das vezes chega ser impossível. Em alguns apps e redes socais há a possibilidade de “postar” uma foto ou vídeo ele fica disponível por 24 horas, após isso é automaticamente apagado, mas na verdade, ele só não fica mais disponível para visualização. Outro caso é enviar fotos intimas, o usuário pode apagar a mensagem caso queira, mas essa foto independentemente se foi removida, fica salva no servidor.

Nunca sabemos com quem lidamos:

- Isso é um fato que é verídico até para quem nós conhecemos pessoalmente, mas na internet fica um pouco pior, pois se já é difícil conhecer alguém que você tenha proximidade, imagine saber como é a pessoa com quem se está lidando, é quase impossível descobrir isso por que o indivíduo se encontra “do outro lado da tela”.

Sigilo em perigo:

- Como foi dito anteriormente, os dados podem ser facilmente encontrados mesmo que não tenha sido disponibilizado para todos, por isso ressalvo que tenham muito cuidado com o que é informado nas redes sociais, porque pequenos acontecimentos que são mostrados lá, podem acarretar riscos aos usuários.

Plágio e quebra de direitos autorais:

- Copiar e distribuir qualquer informação que tenha sido elaborada por outra pessoa sem a autorização ou mesmo sem mencionar a fonte de onde foi tirado tais dados, podem ocasionar processos e até mesmo prejuízos financeiros consequente de processos.

Crimes mais ocorridos e famosos na Internet

Roubo de identidade (Identity theft)

Esse crime também é conhecido no Brasil como falsidade ideológica, que na qual a pessoa se passa ser outra, usando foto, nome e outros dados pessoais falsos para enganar e se aproveitar de outras pessoas. O que é conhecido nas redes sociais como o famoso “fake”.

Como saber se fui vítima desse crime?

Alguns detalhes devem ser analisados e caso um desses problemas que serão listados acontecer com você, tenha cuidado e vá procurar ajuda o mais rápido possível. Esses são algumas situações a qual devemos nos preocupar:

- Dificuldade ou problemas com órgãos de proteção ao crédito, empréstimos ou financiamentos;
- Respostas de e-mails nas quais não houve contato com remetente.
- Acesso indevido de redes socias, e-mails, em locais e horários na qual não é frequente o login e tenha sido tentado pelo dono da conta.
- Anormalidades em sua conta bancária, preste atenção no que conta no seu extrato bancário, e recorra ao banco caso haja algo que tenha sido efetuado por você.
- Ligações, e-mails, correspondências e até mesmo cobranças que o assunto não condiz a você, no caso de cobranças, compras que tenham sido efetuadas em locais e horários diferentes na qual não foi você quem a realizou.

Como se prevenir?

Ações como essas podem prevenir de ter a sua identidade ou seus dados roubados:

- Usar criptografia em seus e-mails;
- Usar sites na qual possuam HTTPS;
- Jamais passe informações e dados pessoais a terceiros, e não deixe suas informações salva em aparelhos de outras pessoas;
- Uso da guia ou identidade anônima que é disponibiliza nos browsers;
- Tenha cautela com o que divulgado a seu respeito nas redes sociais: telefone, informações pessoas, localização, local de trabalho;
- Use VPN, para “mascarar” sua localização.

Fraude de antecipação de recursos

A fraude de antecipação de recursos, ou advance fee fraud, é aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

Comitê Gestor da Internet, 2012, pág. 07

Esse tipo de crime é muito conhecido por todos nós, a ainda é muito praticado, principalmente por presidiários que se passam por funcionários de diversas companhias e dizem que você ganhou alguma quantia em dinheiro, e pra que ser disponibilizada, um depósito precisa ser efetuado em uma conta fornecida por esse criminoso. Houve também casos famoso de que há a simulação de sequestros.

Como se prevenir?

Desconfie de ligações, mensagens de texto, mensagens em redes socias de desconhecidos, procure sempre estar informado sobre o que ele está falando, tome cuidado, que as vezes eles procuram as informações na internet sobre por exemplo loteria, recarga premiada, para poder te enganar e efetuar o golpe.

Desconfie também sobre o “emprego dos sonhos”, que para ser contratado é necessário pagar algo.

Phishing

Phishing, phishing-scam ou phishing/scam, e o tipo de fraude por meio da qual um golpistatenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Comitê Gestor da Internet, 2012, pág. 09.

Fique muito atento a esse tipo de crime, pois até mesmo celebridades já caíram no mesmo. Tenha cuidado ao acessar sites ou links contidos em e-mails, pois podem ser uma estratégia usada para roubar suas informações, sites de bancos, sites de e-commerce, são os mais visados pelos criminosos, haja com cautela, porque em muitas das vezes esses site são semelhantes ou idênticos ao site verdadeiro na qual você pretende visitar.

Como se prevenir?

- Fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links;
- Questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há porque recadastrar dados ou atualizar módulos de segurança);
- Fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descrito.

Comitê Gestor da Internet, 2012, pág. 11.

Pharming

Pharming é um tipo específico de phishing que envolve a direção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (Domain Name System). Neste caso, quando você tenta acessar um site legítimo, o seu navegador Web é redirecionado, de forma transparente, para uma página falsa.

Este redirecionamento pode ocorrer:

- Por meio do comprometimento do servidor de DNS do provedor que você utiliza;
- Pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do seu computador;
- Pela ação direta de um invasor, que venha a ter acesso às configurações do serviço de DNS do seu computador ou modem de banda larga.

Prevenção:

- Desconfie se, ao digitar uma URL, for redirecionado para outro site, o qual tenta realizar alguma ação suspeita, como abrir um arquivo ou tentar instalar um programa;
- Desconfie imediatamente caso o site de comércio eletrônico ou Internet Banking que você está acessando não utilize conexão segura. Sites confiáveis de comércio eletrônico e Internet Banking sempre usam conexões seguras quando dados pessoais e financeiros são solicitados;

Comitê Gestor da Internet, 2012, pág. 11.

Boato *(Hoax)*

Um boato, ou hoax, é uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental. Por meio de uma leitura minuciosa de seu conteúdo, normalmente, possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides.

Comitê Gestor da Internet, 2012, pág. 15

Todos já devem ter recebido aquelas correntes de redes socias, com uma oferta de emprego de determinada instituição com um alto salário, dizendo que seria o início imediato, pois então, essa é uma forma de phishing ou um hoax que para muitos, realmente é uma oferta de emprego, para ter certeza de que tal empresa está contratando, vá ao site oficial da companhia, e veja se há alguma vaga.

Como se prevenir?

- Fique atento se qual remetente insistir que aquilo não é falso;
- Possíveis ameaças caso não siga o que ele está lhe mandando;

- Promessa de benefícios financeiros;
- Erros de ortografia e gramática;
- Informações contraditórias;
- E no próprio texto, pedir para ser passado adiante.

Esses sites abaixo demonstrar e desmentem os boatos:

Monitor das fraudes: http://www.fraudes.org

Quatro Cantos: www.quatrocantos.com

Ataque de força de bruta (brute force)

Esse ataque é caracterizado pelas tentativas de se acertar determinado login e senha de um usuário.

Qualquer dispositivo que possui esse mecanismo de login e senha e que esteja conectado à internet pode ser algo desse ataque.

Segundo o Comitê Gestor da Internet no Brasil (2012), alguém que detenha seu usuário e senha pode:

• Trocar a sua senha, dificultando que você acesse novamente o site ou computador invadido;

• Invadir o serviço de e-mail que você utiliza e ter acesso ao conteúdo das suas mensagens e sua lista de contatos, além de poder enviar mensagens em seu nome;

• Acessar a sua rede social e enviar mensagens aos seus seguidores contendo códigos maliciosos ou alterar as suas opções de privacidade;

• Invadir o seu computador e, de acordo com as permissões do seu usuário, executar.

Mesmo que sofrendo o ataque e não sendo bem-sucedido, você poderá ter problemas também, tais como: bloqueio de conta por excesso de tentativas de login, e esse golpe pode ser feito manualmente, ou por meio de programas que geram senhas aleatoriamente.

Portanto, lembre-se sempre de criar uma forte senha forte, e é claro, lembrar da mesma, pois com uma senha utilizando letras maiúsculas, letras, caracteres especiais e números, dificilmente será acertada em um ataque de força bruta. Outro fato importante, não use uma senha e login padrão, pois caso aconteça o pior, e sua senha for descoberta, esse infrator poderá invadir mais serviços nos quais possuem tais informações.

Spam

Os famosos “spans” são e-mails indesejados, ou seja, o destinatário não possui contato algum com o remetente, geralmente esses e-mails possuem algum tipo de link, que em muitos casos podem conter algum “malware”, esses e-mails são como as “correntes” de redes socias, são enviados para muitas pessoas com o intuito de atingir um grande número de vítimas.

Portanto, caso você receba um spam, notifique ao seu mecanismo de e-mail, e apague essa mensagem sem clicar no link anexado, pois certamente esse link irá direciona-lo para uma página que pode ser nociva para quem acessa-la.

Malware

Malwares são programas instalados e até mesmo alguns links que são noviços para a “saúde” do aparelho, estes softwares tem como objetivo infectar e

danificar o dispositivo na qual ele se infiltra, podendo causar danos como perda de dados, furto de dados, ou até mesmo impedir o funcionamento do celular, desktop, etc.

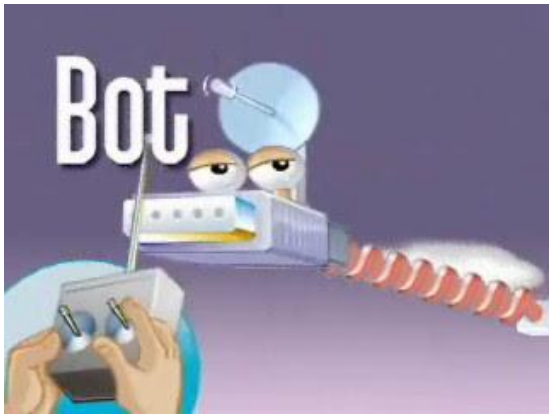
Portanto, tenha cuidado com os aplicativos ou programas que irá instalar, procure sempre baixar os softwares de locais ou sites seguros, e fique atento com links que são repassados pelas redes sociais, ou até mesmo por e-mails, com os famosos “spam”, porque uma vez que o malware se tem acesso ao seu aparelho ou máquina, os danos podem ser cruciais para o bom funcionamento deles.

Vírus

Os vírus são um tipo de malware, porém, para ele causar dano para o usuário ele precisa ser executado, ou seja, ele é como um programa que você instala em sua máquina ou dispositivo, após ser executado, ele faz cópias de si mesmo e vai infectando outros arquivos e programas até tomar conta de tudo. Existem várias categorias de vírus, dentro delas estão:

- **Worm:** é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

- **Bot e botnet:** é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente.



- **Spyware:** é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Os mais conhecidos são:

Keylogger: capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.

Screenlogger: similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado.

- **Backdoor :**é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

- **Cavalo de troia, trojan ou trojan-horse:** é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Por que há tantos golpes na Internet?

Segundo o Globo, golpes bancários pela internet tiveram o aumento de 297% em um ano, em 2016 o número de queixas registradas foram de 425, e em 2017 o número aumento parou 1688 reclamações.

Mas por que há tantos golpes? Primeiramente porque há pessoas más intencionadas e que possuem habilidade em computação, criptografia, engenharia social, e persuasão para enganar as pessoas e se beneficiar com isso. A falta de leis rígidas e rigorosas contra esse tipo de infrator é um dos motivos nos quais muitos usam seus talentos para o mau, e a dificuldade de rastreio é outro fator que os chama atenção, pois em muitos casos, eles agem sem deixar rastros.

O fato de que há pessoas desinformadas sobre os perigos que a internet possui é outro fato de suma importância, muitos usuários são os famosos “usuários básicos”, que apenas usam a internet para redes socias e pesquisas, esses são os principais alvos de criminosos, outro fato redundante, é que muitos acham que aquilo nunca acontecerá com eles, e essa ignorância junto com a ganância de uma oportunidade de ganhar dinheiro facilmente, acaba os atraindo para o “buraco”.

A maioria dos sistemas de segurança de bancos online são seguros, sabendo disso os infratores buscam atingir os clientes das agências, sabendo que ali é onde se encontra a fragilidade e aproveitam da situação.

Como posso me proteger?

Simples ações podem lhe ajudar a não ser vítima de um ataque virtual, elas não uma garantia de 100% que você está seguro, mas irá lhe ajudar e muito a se prevenir, estas dicas são:

- Usar softwares e programas originais;
- Sempre verificar se seus programas possuem alguma atualização, pois com elas, falhas e erros são corrigidos e sendo assim o programa fica melhor;
- Atualizar o seu sistema operacional, isso mesmo, simples e muito prático essa dica;
- Usar um sistema operacional original, pode até ser caro, mas veja isso como um investimento de segurança, ou se preferir, use um sistema operacional diferente com menos probabilidade de ser hackiado;
- Deixe sempre seu firewall ativado, pois ele impede que outros usuários invadam seu dispositivo;

- Use antivírus, assim como o firewall, ele também impede a presença de pessoas sem autorização de invadir seu aparelho, além de protege-lo contra vírus.
- Navegue sempre em sites confiáveis e seguros, que usem HTTPS;
- Use a guia ou janela anônima disponível em seu browser;
- Tome cuidado com e-mails desconhecidos;
- Não clique em qualquer link que seja suspeito ou enviado por desconhecido;
- Jamais compartilhe sua senha e seu login com outras pessoas;
- Jamais informe seu número de cartão de crédito para terceiros;
- Desconfie de ligação, mensagens e e-mail com oferta de emprego e de produtos sensacionais;
- Não deixe sua senha e login salvo em aparelho público ou de terceiros;

Bom, espero que tenha lhe ajudado com essas dicas, e espero que a partir da leitura você tome mais cuidado com o que faz na internet, porque além dos benefícios, ela pode te trazer prejuízo se mau usada.

REFERÊNCIAS

Comitê Gestor da Internet no Brasil. Cartilha de Segurança para Internet – Versão 4.0. 2 ed. São Paulo: 2012. Disponível em <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em 23 nov. 2018.

DIGITAL IN 2018: WORLD'S INTERNET USERS PASS THE 4 BILLION MARK. Simon Park, 2018. Disponível em < https://wearesocial.com/blog/2018/01/global-digital-report-2018>. Acesso em 22 nov. 2018.

Queixas de golpes bancários por internet crescem 297% em um ano. Gabriel Martins, 2018. Disponível em <https://oglobo.globo.com/economia/queixas-de-golpes-bancarios-por-internet-crescem-297-em-um-ano-22363527>. Acesso em 23 nov.2018.